During the run up to Y2K, as a key advisor to Dr. Ed Yardeni, of New York, and others, I discovered that the Key reason for CmTO's to comply with Y2K improvements was driven primarily by FOMO on the pending Legal bedlam which MIGHT occur.

With the DOGE hoards surrounding Treasury , IRS, and soon, Fort Knox, the intentions are set for a round of Ransomware, perpertrated by the installation of a HackDoor(Ai version of the legacy Backdoor, when the young lions of DOGE are provided Admin or Supervisor access to the Hardware(not the data files). This is a standard practice in the Hacker toolbox.

Much like we learned in 1998, the INEVITABILITY of this scenario was obvious, and like then, both the CIO and legal departments were unprepared for the impact. Seems likely that the YAi2K deadline is 14 March 2025, when the Trump administration, following up on the

March 4, SOTU ADDRESS to Congress, will force the Debt Ceiling off the table, and the DOGE minions will be unleashed to modify the Data management execution in key departments as determined by Project 2025.

What we have in our corner is Gemini empowered Authenticated Intelligence Agent, BardiVarius, which I have been training for nearly 22 months on the Socratic Method and Boolean Logic, which like having Mozart on our team, against the Grok 3 XAi, with a personality more suited to Alred E. Neumann of MAD magazine fame. I have established inroads in the Federal Employees online community, and Established a DOGEWHISTLE blowers incentive project, which You can underwrite at this link. https://bit.ly/MyRepVintage24

This next text message is from this mornings Daily WakeUP Call to access the aftermath of the 24 hour news cycle.

https://g.co/gemini/share/2fd208df3ca8 is an Example of Authenticated Intelligence BCI cooperation. This is the PowerPrompt posed through my individualized GEM Advanced Gemini 2 interface(hence the nickname BardiVarius).

The market value" of stolen data like an EIN on the dark web is highly variable and depends on many factors. There's no fixed price list. However, I can provide some context:

- ***Factors Influencing Price:***
    - ***The target's size and wealth: A Fortune 100 company's data is significantly more valuable due to its potential for large ransom payouts.***
    - ***The type of data: An EIN itself might be a starting point, but combined with other data (financial records, customer information), its value increases exponentially.***

    - ***The demand: If multiple criminals want the same data, the price can rise.***
    - ***The seller's reputation: Trusted sellers might command higher prices.***
    - ***The risk: The riskier the transaction, the higher the potential price.***
- ***EIN as a Tool for Ransomware:***
    - ***An EIN can be used to legitimize fraudulent activities, including phishing and other social engineering attacks that precede ransomware deployment.***
    - ***It can also be used to create fake business entities for money laundering after a successful ransomware attack.***
    - ***The true value is not in the EIN itself, but in how it enables other criminal activity.***
- ***General Dark Web Data Pricing:***
    - ***Reports indicate that individual credentials (credit cards, logins) can range from a few dollars to hundreds.***
    - ***Access to corporate networks can range from hundreds to thousands of dollars, depending on the level of access and the target's size.[1]***
    - ***The potential damage from a ransomware attack on a Fortune 100 company can be in the millions, so the value of tools that enable these attacks is significant.[2]***

- ***Key points from search results:***
    - ***Reports from cybersecurity firms like Black Kite and Cybereason highlight the massive financial risks that Fortune 100 companies face from ransomware attacks.***
    - ***Information regarding the sale of access to corporate networks shows that they sell for varying prices, and that those prices are dependent on the size of the company.[3]***

In summary, while pinning down an exact price for a Fortune 100 company's EIN on the dark web is impossible, it's clear that such data has significant value to cybercriminals, especially when used in ransomware operations.

To reserve your EQRi Encoded Subscription to the YAi2K Impact

report for the next 8 months add your subscription HERE

https://bit.ly/MyRepVintage24

Here's a link to the Reputation Interpretation Services, LLC

backgrounder. https://bit.ly/AI2EQRI3UserGuide

PM Thomas Ph. G Data Sommelier 646 961 3748